INFERENCING DATA TYPES OF MESSAGE COMPONENTS

ABSTRACT OF THE DISCLOSURE

[0092] A security gateway receives messages and extracts components thereof, typically in the form of field name-value pairs. The security gateway determines a data type of the values for individual field names to infer the most restrictive data type of the values for that field. The security gateway may then generates rules, which would block messages that do not have values that match the most restrictive data type. Since the most restrictive data type defines a data type of values for the field as narrowly as possible, the generated rules will make it more difficult for an intruder to guess a valid data type of a value. Since messages that have values that do not match the most restrictive data type are likely to represent malicious attacks, the more narrowly the data type of values is defined, the greater the number of illegitimate messages that will be blocked.